

**GOVERNMENT OF ANDHRA PRADESH
ABSTRACT**

ITE&C Department – AP Policy on Unique Identification of Residents - Orders – Issued.

INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS (eGov) DEPARTMENT

G.O.MS.No. 16

Dated:29.07.2015

ORDER:

The Government of Andhra Pradesh envisages *“establishing a system of uniquely identifying the persons normally resident in the State, by assigning an identification number to each, following such process as may be prescribed”*. For this purpose, *“any existing databases, meeting the requirements are to be specified, with the required safeguards”*. Such a system of unique identification of residents introduces efficiency and effectiveness in all the beneficiary-oriented developmental schemes, besides serving several other purposes where identification of an individual is a critical part of the process.

This policy titled **“The Andhra Pradesh Policy on Unique Identification of Residents”**, provides for the system of identification of residents using Aadhaar, the manner of creation, maintenance and usage of Aadhaar for the notified purposes and the establishment of an Aadhaar-Enabled Ecosystem to provide data and application services.

The vision of Aadhaar-Enabled Ecosystem is to establish a secure, reliable and scalable IT infrastructure, processes and platforms to provide a wide-range of identity-related data and application services, and to enable the departments and agencies of the Government to leverage Aadhaar to serve the residents efficiently, effectively and equitably.

However, no person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible or entitled, as per the prescribed criteria.

2 Objectives of the Policy

The Aadhaar-Enabled Ecosystem shall serve the following objectives, in furtherance of the realization of its Vision.

- a) to establish and maintain the State Resident Data Hub (SRDH) as a repository of the Aadhaar data relating to the residents of the State;
- b) to provide data services to the departments and agencies of the Government, relating to seeding of Aadhaar in their databases, authentication of beneficiaries of schemes with reference to the Aadhaar database and cleansing, updation and validation of their databases;
- c) to facilitate creation of a wide-range of Aadhaar-enabled applications that leverage all the benefits envisaged through use of unique Identity of residents, including transfer of social benefits;
- d) to develop tools for online data analytics for planning and decision-support;
- e) to play a pivotal role in the realization of the Vision of AP State Enterprise Architecture, by acting as the People Hub.
- f) To eventually replace all the personal identification numbers and act as the Single ID at all interfaces of the residents with the public and private sectors.

3 Benefits of Aadhaar Enabled Eco-system

The Aadhaar-Enabled Ecosystem shall help the State derive the following benefits.

a. Benefits to the Residents of the State:

- a) All the schemes and benefits of the Government for which a resident is eligible can be accessed directly through an Aadhaar-based single-sign-on facility to be offered by the AEE;
- b) Identity of the residents required at all touch points with the Government, can be made hassle-free by the use of Aadhaar card or through other modes of verification of Identity of the residents;
- c) All the changes in the Government records necessitated due relocation of the residents within the State, temporarily or permanently, can be handled in one stroke, through creation of appropriate application under the aegis of the AP State Enterprise Architecture, obviating the need to approach multiple government agencies at the place of relocation.

- d) Aadhaar-enabled applications will reduce the data/ document burden on the citizens, by storing and reusing the historical, event-related data of the resident, in sectors like education and healthcare, and using it when required.
- e) Aadhaar-enabled Repository of Certificates will obviate the need for the residents to produce proof of various socio-economic attributes, repeatedly at different touch points with Government, leading to a 'Certificate-less Governance'.

b. Benefits to Government Departments & Agencies:

- a) Departments and agencies of the Government can achieve better, quicker and more transparent process of targeting of their benefit schemes, leading to more effective implementation;
- b) The scope for duplicate or non-existent beneficiaries gets eliminated, thus enabling the Government to save precious resources, which can be used for helping more number of eligible beneficiaries;
- c) The process of beneficiary verification and selection gets expedited;
- d) Departments can make use of Data Analytics services offered by AEE to achieve better planning and decision-making.
- e) Government can design integrated and joined-up services to the residents using Aadhaar as the integrating element.

4 Stakeholders of AEE

The following groups shall be the stakeholders of the Aadhaar-Enabled Ecosystem.

- (1) Residents of the State
- (2) Departments and Agencies of the State Government
- (3) Departments and Agencies of the Central Governments
- (4) Banks and Financial Institutions operating in the State
- (5) Service Providers engaged in the delivery of public services, including Village Level Entrepreneurs under the Scheme of Common Service Centre
- (6) Private Institutions operating in the areas of Healthcare, Education and Social Services
- (7) ASAs, AUAs, KSAs and KUAs operating in the State
- (8) Business Correspondents of commercial banks
- (9) The ecosystem of technology companies, device manufacturers, solution providers, innovators and startups.

5 Components of AEE

The Aadhaar-Enabled Ecosystem consists of the following subsystems. The benefits of AEE can be realized only through an orchestrated and coordinated function of these components.

- 5.1 **The State Resident Data Hub (SRDH) or the People Hub:** The State Resident Data Hub (SRDH) or the People Hub is the heart of the AEE. It hosts the near-real-time Aadhaar Data of all the residents of the State in a secure environment. It is the Single Source of Truth in relation to the identity of the residents of the State. All the services envisioned under AEE flow from the SRDH. The positioning of People Hub as a critical component of the APSEA shall also depend on SRDH.
- 5.2 **Aadhaar Data Services System:** Aadhaar Data Services System is an application system that delivers a wide-range of services relating to accessing and use of Aadhaar data available in the SRDH to the stakeholders. It acts as the single interface to the entire ecosystem in so far as Aadhaar Data Services are concerned.
- 5.3 **Aadhaar-enabled Application Services System:** Aadhaar Application Services System is a suite of software applications that can be used by the authorized stakeholders to realize the benefits envisaged by the AEE.
- 5.4 **Aadhaar-enabled Devices Ecosystem:** Aadhaar-enabled Devices Ecosystem consists of a number of initiatives for developing low-cost, affordable devices, especially, those used at the delivery point and establishing the standards therefor.

6 Role, Responsibilities and Architecture of SRDH

6.1 Role and responsibilities of SRDH:

SRDH shall play the following role in AEE.

- a. SRDH shall act as the intermediate facility between the original Aadhaar Data created and maintained by the UIDAI at the Central ID Repository on the one side and the Stakeholders of AEE on the other side.
- b. SRDH shall provide the data support required for the other 2 subsystems namely, the Aadhaar Data Services System and the Aadhaar Application Services System.
- c. SRDH shall decrypt the incremental Aadhaar data received from UIDAI at the defined frequency and update the Aadhaar data present with it .
- d. SRDH shall establish the IT and network infrastructure to enable it to discharge its responsibilities efficiently, complying with the relevant Service Level Agreements.

- e. SRDH shall establish a comprehensive Information Security Management System (ISMS) in compliance with the International and National Information Security Standards.
- f. SRDH shall publish or register its services as web services, to the extent permitted by technology, so as to facilitate consumption of services by the Stakeholders.

6.2 Functional Architecture of AEE & SRDH:

- a. An indicative functional architecture of AEE, including SRDH, is provided in **Annexure I**.
- b. The Architecture of AEE shall be fully compliant with the AP State Enterprise Architecture.
- c. The SRDH shall be hosted in the AP State Data Centre and shall be scalable, secure, and without a single point of failure.

7 Aadhaar Data Services System

Aadhaar Data Services System shall provide the following data services.

7.1 Aadhaar Seeding Service:

7.1.1 Aadhaar Seeding is the process by which Aadhaar numbers of residents are included as a data field in the service delivery database of the Government department or agency or of the service providers. Aadhaar seeding leads to de-duplication of the database and Aadhaar-based authentication during the service delivery. Residents not having Aadhaar shall be encouraged to enrol themselves for getting Aadhaar. In such cases, the departments may adopt other modes of verification of the identity of the residents.

7.1.2 Aadhaar Seeding process is of two types.

- i. **Organic Seeding of Aadhaar:** In this method, the Aadhaar numbers of the beneficiaries are collected through a door-to-door survey or at point-of-sale. Alternative methods are collection of Aadhaar number through IVRS, SMS or drop boxes. Departments with large databases can also engage 3rd party service providers.
- ii. **Inorganic Seeding of Aadhaar:** In this method, the demographic data of the departmental database is matched with that of SRDH through a computer algorithm, and wherever the degree of matching exceeds a threshold level

defined, the Aadhaar number of the resident as in SRDH database is included in the departmental database.

7.1.3 **Annexure II** describes the pre-requisites for Aadhaar seeding, the precautions to be taken in seeding to avoid mistakes and the Standard Operating Procedure (SOP) for effective seeding.

7.1.4 **Convergence of demographic data:** The AEE envisages the ideal situation, where the demographic data contained in the departmental data base and that contained in the SRDH match in all respects, namely, the data definition and data content. Such an envisaged situation will facilitate more efficient processing of service requests and establishing of identity and addresses of the residents. The following principles are laid down in this regard for all departments to comply.

- (i) The demographic details of a resident in the departmental database shall be based on any statutory document like the birth certificate, school or college certificate or degree or passport, if such a document or online information is available.
- (ii) If the demographic details specified in the Aadhaar differ from the data based on such documents as in (i), the resident shall be advised to get the Aadhaar data corrected by preferring an application at the Mee Seva Counter or online.
- (iii) In case the resident does not have any documentary support, and there are differences in the departmental data and the Aadhaar data, the later prevails and the departmental database shall be modified accordingly.
- (iv) The convergence of the demographic data in the departmental database and SRDH shall be realized by all the departments within a period of 12 months of approval of this policy.
- (v) The convergence may be undertaken preferably after the percentage of seeding and its verification crosses 80.
- (vi) The convergence shall be undertaken as a part of the Smart Pulse Survey, described in **Annexure III**.

7.2 Aadhaar Updation Services

- 7.2.1 Aadhaar updation service is provided directly by UIDAI, through Self Service Update Portal (SSUP) and through permanent enrolment centres at Mee Seva outlets. Residents can update Name, Address, Gender, Date of Birth and Mobile number through SSUP portal/MeeSeva Permanent enrolment centres. However changes in Biometrics (Finger print, Photo and IRIS) and all 'Non-Consent cases" can only be updated through Mee Seva Permanent enrolment centres. The resident can also update the above mentioned fields through Postal mode and the Aadhaar Mobile Update facility provided by UIDAI.
- 7.2.2 AEE shall have links to UIDAI Portal for updation, besides the responsibility to undertake periodic awareness programs for continuous updation of data by the residents.
- 7.2.3 AEE shall also be integrated with the AP State Enterprise Architecture in such a manner that life-cycle events such as birth, death and migration trigger consequential changes in all the related databases of residents.

7.3 Aadhaar Authentication Services:

- 7.3.1 Aadhaar Authentication Service is useful to establish that the individual is really the person he/she claims to be. The authentication is useful especially at the time of making financial payments to residents.

Depending upon the importance and sensitivity of the usage, authentication can be of 5 types of increasing sophistication as described below.

Type 1 Authentication- Through this offering, service delivery agencies can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc.) of a resident.

Type 2 Authentication- This offering allows service delivery agencies to authenticate residents through One-Time-Password (OTP) delivered to resident's mobile number and/or email address present in CIDR.

Type 3 Authentication- Through this offering, service delivery agencies can authenticate residents using one of the biometric modalities, either iris or fingerprint.

Type 4 Authentication- This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.

Type 5 Authentication- This offering allows service delivery agencies to use OTP, fingerprint & iris together for authenticating residents.

The Aadhaar number needs to be submitted in all forms of authentication so that this operation is reduced to a 1:1 match. Aadhaar number itself is not an authentication factor. Type 1- authentication may be combined with any other Aadhaar authentication offering.

Service delivery agencies should select the appropriate authentication type based on their business requirements. They would need to balance out the resident convenience and service delivery risk before deciding upon the type of authentication used in a case.

7.3.2 Aadhaar Authentication Ecosystem

- a. The ecosystem established by UIDAI will be used for Aadhaar authentication. The ITE&C Department, Government of Andhra Pradesh is functioning as AUA-ASA and KUA-KSA with UIDAI. The departments of the State can engage their department as a Sub AUA-ASA with ITE&C department, to utilize authentication services. The format of the agreement that the departments should sign with the ITE&C Department for providing the authentication services can be accessed at <http://srdh.ap.gov.in/andhrasrdh>-- Please see AUA Agreement tab).
- b. All the departments of the Government that deal with beneficiary/citizen oriented e-Governance schemes, involving over 10 lakh beneficiaries are required to enter into agreement with ITE&C Department within a period of 12 months from the notification of this policy.
- c. All other departments and agencies that deal with beneficiaries and deliver citizen services shall enter into an agreement with ITE&C department within 2 years.
- d. The departments specified in (b) & (c) above shall take up capacity building programs in coordination with the ITE&C Department or the agencies nominated by it.

- e. A robust system with high availability & scalability for biometric authentication (both Fingerprint & Iris) will be designed to deliver citizen services. To avoid denial of service and guaranteed service at any point of time at all the department touch points for the residents (in case of connectivity issues or low quality biometrics of citizens due to age factor or Aadhaar server non availability or any gap in AUA-ASA-UIDAI process) appropriate fallback mechanisms shall be designed by respective departments and adopted.

8 Aadhaar-enabled Applications System

- 8.1 Aadhaar-Enabled Applications System (AEAS) provides a development environment which facilitates development of applications which have the central functionality of identification of residents, by the departments and application service providers.
- 8.2 AEAS shall also design, develop and host a suite of standard applications that can be used by the departments and application service providers in conjunction with their departmental applications so as to provide a wide-range of value-added services, basing on Aadhaar. 5 of the most commonly required applications, which shall be part of the suite are described in the following sub-sections of this policy.
- 8.3 Application for Establishing Identity: The following modules form part of the Application for Establishing Identity.
 - (i) **Adding New Beneficiaries to departmental database**– This module uses Aadhaar authentication process as proof of identity and proof of address and can be deployed in all beneficiary-oriented schemes. This module can also be used to provide the residents access to social leellers such as financial inclusion and digital inclusion, which have so far been denied to certain sections for want of easy and reliable proof of identity. Also Socio-economic Data of residents is required, to make a practical use of the basic data of Aadhaar demographic data. **Annexure III** explains the methodology for collection of the Socio-economic data.
 - (ii) **Confirming the identity of beneficiary at PoS**– This module can be used in various programs at the point of service delivery or disbursement of benefits, where the identity of the beneficiary needs to be confirmed using Aadhaar authentication. This will help curb leakages and ensure that the targeted beneficiary is not denied entitlement.
 - (iii) **Convergence/Aggregation service**– This module enables the Government to take a 360-degree view of the benefits being given to any resident through

different schemes. Such converged data will result in faster and better decisions in granting the benefit to the resident.

- (iv) **Attendance Monitoring**– This module can be used by Programs in sectors like Education, Welfare and Livelihood, where the implementation is tightly linked to beneficiary attendance. The module uses Aadhaar authentication for attendance monitoring.
- (v) **Access control**– This module enables Aadhaar authentication as a means to control access/ entry to restricted areas such as airports, hotels, examination halls etc.

8.4 **Application for enhancing Efficiency in Service Delivery:** The following modules shall form part of the Application for enhancing Efficiency in Service Delivery.

- (i) **Anywhere Service Delivery:** This module enables the departments to implement the concept of Anywhere Service Delivery, without limitation of jurisdictions of field offices, as the identity of the resident (recipient of service) can be established anywhere through Aadhaar Authentication.
- (ii) **Tracking Service Delivery:** This module enables tracking of a benefit or a request for benefit on an end-to-end basis, and provide transparency both to the department and to the beneficiary. This is achieved by tracking the service request from the time it is received till it is closed, w.r.t the Aadhaar number. If a payment or supply transaction is so tracked, it can curb leakages and diversions of Government benefit.
- (iii) **Accountability & Vigilance:** This module enables to strengthen the accountability in activities relating to audit, inspection and vigilance through Aadhaar-based authentication of the concerned officials along with time-stamping and GPS tracking.
- (iv) **Empowering beneficiary:** This module enables beneficiaries to access government schemes in an integrated manner, to know all their entitlements at one time using Aadhaar Identification. It would also enable them to know the status of their current entitlements, and enable them to lodge grievances in respect of delays or any other matters. These features shall be made available through portals such as Mee Seva and Mee Kosam.

8.5 **Application for verification of Address & demographic details:** The following modules shall form part of the Application for verification of Address & demographic details:

- (i) **Services linked to residence:** Verification of address is a key requirement for the residents to avail many services like applying for a telephone or gas connection, passport, opening a bank account, taking an insurance policy. This module enables the address to be verified using Aadhaar.
- (ii) **Services needing demographic information:** Several services of the Government require proof of demographic details like the age or date of birth. This requirement can be avoided by use of Aadhaar.
- (iii) **Notifying Change of Address:** Aadhaar can act as the single point of reference for the current address of a resident. Whenever the address changes due to migration, relocation etc, the change is requested at the respective Mee Seva Centre or online. Change of address in Aadhaar data base should suffice for all government agencies of central and state government and for utilities and service providers to know the changed address.

8.6 Aadhaar e-KYC Application: A fundamental building block for service delivery is the KYC (Know Your Customer) process, which establishes the identity of the resident, their address, and other basic information such as their date of birth and gender. Typically, this KYC information is combined with other information at the point of service delivery to determine eligibility – either for an LPG connection, a scholarship, a loan, a social security pension, a mobile connection, etc.

The Aadhaar e-KYC service provides an instant, electronic, non-repudiable proof of identity and proof of address along with date of birth and gender. In addition, it also provides the resident's mobile number and email address to the service provider, which helps further streamline the process of service delivery. e-KYC may be performed at an agent location using biometric authentication, as well as remotely using an OTP on a website or mobile connection.

The Aadhaar e-KYC ecosystem has been designed to be scalable, just like the enrolment, updations, and the authentication ecosystems. It follows the same operating model as that of the Aadhaar authentication ecosystem.

Annexure IV gives the salient features of the Aadhaar e-KYC Service.

8.7 Aadhaar-enabled Payment Systems: With Financial Inclusion receiving increasingly higher priority of the Government, the environment for making payments to beneficiaries

under various schemes of Central and State Governments shall become more transparent, efficient and effective. This is made possible in the Aadhaar-enabled Payment System (AEPS), by using Aadhaar for identification and authentication. The components and functions of AEPS are described in **Annexure V**.

9 Aadhaar-enabled Devices Ecosystem

- 9.1 **Device Ecosystem:** In order that the entire AAE works efficiently, a device ecosystem compatible with Aadhaar ecosystem shall be put in place. The Aadhaar-enabled access devices shall have the features for demographic authentication, biometric authentication (finger print, iris or both), mobile connectivity, memory and processing capacity, as per the standards and specifications to be laid down by the UIDAI and the Government of Andhra Pradesh.
- 9.2 **Conformance Testing:** The Aadhaar-enabled devices shall be certified for compliance with the specifications and standards, by the certification bodies to be notified by the Government in this regard.
- 9.3 **Research & Development:** The AP e-Governance Authority, in association with the R&D Institutions at the national level, and the UIDAI, may undertake research in areas relating to standards, protocols and specifications of the devices, in particular and other components in general, that can form part of the Aadhaar-Enabled Ecosystem as also the design and development of low-cost devices.

10 Governance Structure

The Aadhaar-Enabled Ecosystem shall be administered by the ITE&C Department of the Government of Andhra Pradesh.

10.1 Organization Structure: The AP e-Governance Authority, a Society established by the ITE&C department shall be made responsible for the implementation of the scheme of AEE. For this purpose, the APeGA shall establish a Division with responsibilities defined for establishment and management of the 4 components of the AEE specified in Section 6. The APeGA shall enter into anMoU with the ITE&C department, to detail the specific activities it shall undertake, the timelines, standards and SLAs that it shall comply with.

10.2 Budget : The Government of Andhra Pradesh shall provide budgetary resources to the APeGA, to enable the later to discharge its responsibilities effectively. The APeGA shall also be authorized by the Government to collect service charges at rates to be specified by the

Government for various services it renders to the departments and agencies of the Government and to the service providers in the private sector.

10.3 Coordination: The Government of Andhra Pradesh, through its ITE&C Department shall coordinate with the UIDAI in the course of implementing the scheme of AEE, so that the developments at the national level are factored into AEE and the benefits are thereby enlarged and in alignment with the national standards and protocols.

11 Security and Privacy

All the authorities in possession of the personal information of residents shall undertake safeguards and measures specified in **Annexure VI**, while collecting, storing, dealing with or handling such information, so as to ensure the security and privacy of such information.

(BY ORDER AND IN THE NAME OF THE GOVERNOR OF ANDHRA PRADESH)

B. SREEDHAR,
SECRETARY TO GOVERNMENT

To
All the Departments of Secretariat
All the District Collectors & Magistrates, AP
All the HoDs
The Managing Director, M/s APTS Ltd.
The CEO, APeGA

Copy to:
The Chief Minister's Office/Chief PRO to C.M.
The OSD to Hon'ble Minister for Information Technology, Andhra Pradesh
The PS to Hon'ble Minister for Finance, Andhra Pradesh
The PS to PFS, Andhra Pradesh
The PS to OSD to Hon'ble CM, Andhra Pradesh
The PS to Chief Secretary to Government of Andhra Pradesh

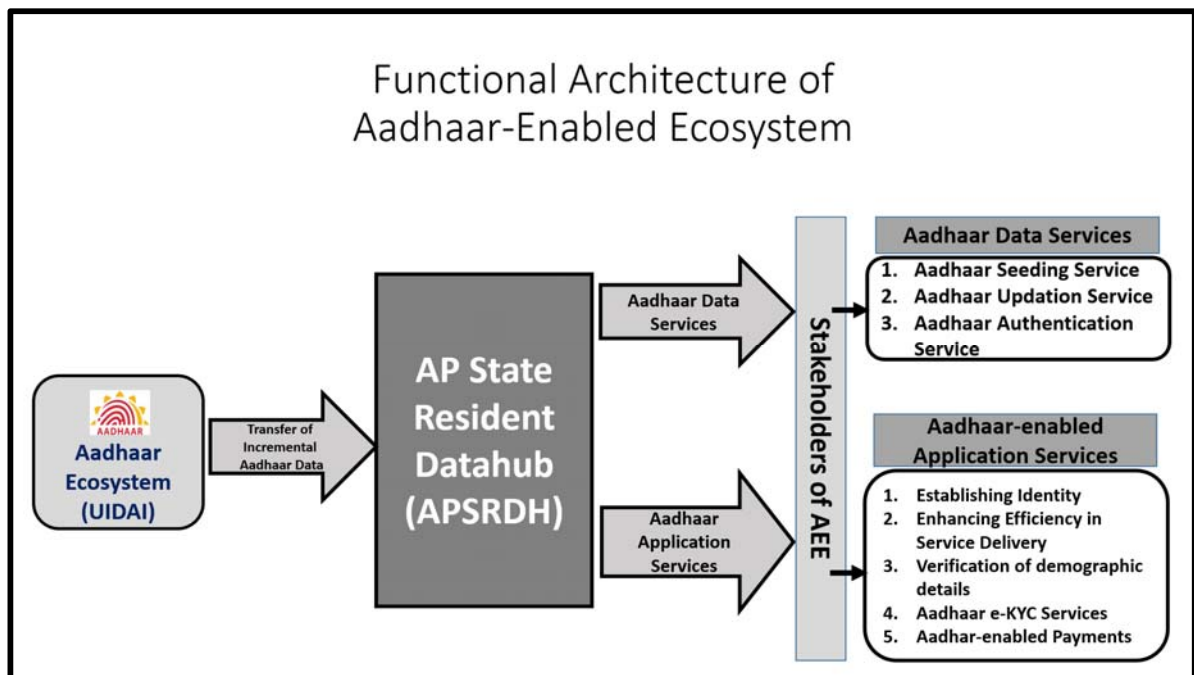
//FORWARDED :: BY ORDER//

SECTION OFFICER

Annexure I

Functional Architecture of Aadhaar-Enabled Ecosystem

(PI See Section 7.2)



Annexure II

Aadhaar Seeding

(Pl see Section 7.1.3)

II.1 Pre-requisites for Aadhaar Seeding

In order to initiate the process of Aadhaar Seeding in any departmental database, the following pre-requisites must be satisfied:

1. **Digitization** of existing beneficiary data which may currently exist either in distributed databases, or in manual registers.
2. The application software managing the scheme or service should be based on a **centralized architecture**.
3. **Aadhaar Enrolment of beneficiaries**. All the beneficiaries should have an Enrolment ID (EID) or Aadhaar number.
4. Provision shall exist in the departmental database to include Aadhaar number **field** with the following checks in-built in software:
 - a. Aadhaar number will always consist of 12 digits
 - b. Aadhaar number cannot start with 0 & 1
 - c. The structural validity of each Aadhaar number should be checked by use of Verhoeff algorithm (URL: http://en.wikipedia.org/wiki/Verhoeff_algorithm)
5. The EID Number should only be used to fetch the corresponding Aadhaar number from SRDH.

II.2 Standard Operating Procedures (SOP) for Aadhaar seeding

- i. Andhra Pradesh State Resident Data Hub (APSRDH) is a repository of Aadhaar demographic data along with photographs of residents enrolled for Aadhaar and to be used for seeding by various Govt. departments for various benefits schemes.
- ii. To seed Aadhaar numbers against their beneficiaries, Departments can utilize APSRDH or existing departmental application. If the department chooses to use their portal to seed Aadhaar, the department can utilize the web-service provided by APSRDH to pull the demographic data along with photo of the resident.
- iii. Various applications in department can use the web-service provided by APSRDH for pre-populating Aadhaar information and should implement the following in the department portal for Aadhaar Seeding:
 - a. **Verhoeff Algorithm** – to check the number validity of entered Aadhaar number. If the entered Aadhaar number is not valid as per the Verhoeff algorithm, the department application should not allow its seeding.
 - b. **Check for Cancelled Aadhaar number / Rejected Enrolment Identity number (EID)** – Using the web service provided by SRDH, the departmental application

shall check whether the Aadhaar number or EID number entered has been cancelled or rejected respectively. In such cases, the application should not allow its seeding.

- c. **Aadhaar number is valid but demographic details are not available with APSRDH** – In such cases, the application should allow entering the demographic details as in Aadhaar card or reading the Hologram in Aadhaar card through Aadhaar Card reader App and adopting the relevant web service provided by SRDH.
- d. **Aadhaar number is valid but demographic details are not available due to Non-Consent** – In such cases the department should encourage the beneficiary to change his/her Non-Consent to Consent at nearest permanent Aadhaar enrolment centers using the eKYC service.

Fig II.1 Verification of Demographic data – Example of a Success case

- iv. After the seeding is done either in departmental application or in APSRDH the demographic authentication needs to be performed on the seeded records. APSRDH will perform bulk demographic authentication and provide SUCCESS or FAILURE results. A web service is also provided by APSRDH to perform bulk demographic authentication with Aadhaar server through AUA-ASA link. Departments can also make use of this facility from APSRDH by entering into a sub-AUA agreement with ITE & C Department, Govt. of Andhra Pradesh.
- v. A real time synchronization has to be established by the department with APSRDH. This will help to incorporate the incremental beneficiary details in the departmental database.
- vi. After demographic authentication, the designated department official verifies the demographic authenticated failure cases and can either APPROVE / REJECT them by following the procedure as follows:
 - a) Compare the beneficiary's data in department with seeded Aadhaar data provided by APSRDH.
 - b) Decide whether both data belong to the same person.

- c) Accept the seeding request if both the data matches
- d) Reject the request if there is a mismatch.

Department : Civil Supplies District : EAST GODAVARI Mandal : AMALAPURAM Village : A. VEMAVARAM

Seeded Record

UID Details		Civil Supplies Details	
UID	695647127709	Scheme ID	WAP045404900143
EID	1055553230117920110223105634	Unique ID	WAP0454049001434
Name	Ketha Sujatha	Beneficiary Name	Pavan Kumar
Care of Name	D/O Ketha Mohan Marthand	Care of Name	Ketha Mohan Marthand
Date of Birth	06/05/1995	Date of Birth	01/01/1989
Building Name	4-98/2	Building Name	4-98/2
Gender	F	Gender	M

Fig II.2 Verification of Demographic data – Example of a Failure case

- vii. The rejected data will be re-validated by collecting correct Aadhaar number as explained in steps i to v.
- viii. A Biometric authentication has to be performed on the demographic success data and department can make use of AUA-ASA facility with CIDR as a web service through APSRDH.
- ix. For cases where there is a name mismatch between Aadhaar and beneficiary data, department should encourage the beneficiary to correct the data after performing demographic and biometric authentication. If the data in Aadhaar is incorrect, the beneficiary should approach the permanent enrolment centers established in each mandal to correct the demographic data or can apply online (<https://resident.uidai.net.in/update-data>). In case, the demographic data is incorrect in the department then the department should adopt the Aadhaar data after demographic and biometric verification.
- x. The department should build a mechanism in the POS machine to perform both demographic and biometric authentication for proper seeding of Aadhaar and disbursement of welfare benefits.
- xi. Proper Capacity building programs have to be taken up by the department to impart training to the Seeders and Verifiers.

Annexure III

Socio-economic data collection through Smart Pulse Survey

(Please see 7.1.4)

For any database to be relied upon by the Enterprise as a Core Data, it has to be Authentic, Reliable, Consistent, Real-time, standards-based and Technologically sound. Aadhaar stands well on all these grounds except the first attribute namely, authenticity, since the data collection and entry was done through private agencies. However, this lacuna can be cured through field verification by the Revenue authorities.

Andhra Pradesh has already created a State Resident Data hub (SRDH) in association with the UIDAI. The SRDH mirrors the Aadhaar data relating to AP from the Data Repository of UIDAI in Bangalore/ Manesar. The data is updated at a defined periodicity. The Basic Data on any resident that Aadhaar has, contains the fields Unique Aadhaar Number, Name, C/o Name, Date of Birth or Year of Birth, Gender, Address, Postal PIN code, Photo, Biometric data (10 fingerprints + Iris). While UIDAI has shared the demographic data elements, the biometric data is available for a case-to-case online biometric authentication.

Departments of GoAP have undertaken a massive drive of seeding of Aadhaar in all major departmental databases which is likely to be completed soon. However, the aggregate of data entered by the departments falls short of the socio-economic data requirements. In view of this, the best strategy is to take the data aggregated by the Aadhaar Number as the basis of the Smart Pulse Survey, and to do appropriate gap-filling to create the core People database.

There are two methods to collect the socio-economic data of an individual w.r.t. his / her Aadhaar number:

Method 1:

Seeding of Aadhaar in the databases of all the socio-economic development programs of the Government, by matching records w.r.t. place of residence and name. This can be tedious and time consuming.

Method 2:

Conduct **Smart Pulse Survey**, which is a massive parallel survey of all households, and capture the required socio-economic data directly in digital form, with online validations. The field surveyors can enter the data by accessing the relevant portal through a connected tablet so that

- i. the data validations happens on the fly and the scope for mistakes is minimized and
- ii. the consolidation and analysis of data can be completed within 2 weeks of the completion of field survey.

Data Updation Methodologies: This section explains the methodologies recommended to update the basic Aadhaar demographic data and Socio-economic data.

- i. **Aadhaar Basic Demographic Data:** A combination of 3 methods is recommended to keep the basic (Aadhaar) data updated with SRDH:
 - a) A near real-time mirroring of SRDH with the Aadhaar database may be attempted;
 - b) The permanent Aadhaar Enrolment Centres (PEC) already established in all Mandal Offices in the State, may be activated so as to provide opportunity for those not enrolled already to register themselves, and to record changes resulting from births and deaths. All PEC's to have a bio-metric device for performing Bio-metric Authentication & e-KYC services.
 - c) Live links may be provided to the registers of marriages, births and deaths to receive notifications that can trigger changes in the SRDH, via the Aadhaar enrolment process.
- ii. **Socio-economic Data:** A combination of 3 methods is recommended for ensuring that the socio-economic data is kept updated on a continuous basis with SRDH.
 - a) A real-time link is established between the SRDH and all the domain databases dealing with people, be it for disbursement of benefits, for providing health and education services or for transacting any work with the Government. The changes in the socio-economic profile of the individual impacting the 'additional' data, if any, are captured and the additional data in the SRDH is updated.
 - b) The additional data in SRDH may be used to provide access to selected G2C transactions so as to identify any changes and trigger action to verify and authorize the changes to the SRDH.
 - c) It may also be necessary, for a Smart Pulse Survey to be conducted on a single day once a year, to update the additional data. Such an annual survey can be

conducted 3 times, by which time all the SRDH-based systems are expected to stabilize and get internalized.

The instrument to be canvassed during the Smart Pulse Survey, and the processes associated with it shall be so designed as to identify benami records, ineligible beneficiaries and grievances of the people, which need to be addressed in a closely monitored manner. Given the complexities, it is desirable to conduct the Smart Pulse Survey in ONE District at first.

Data Standards: The following Standards are to be followed in respect of the Core Data of People.

- a) The Metadata and Data Standards (MDDS) followed by UIDAI while designing the Aadhaar database schema may be adopted as the de facto standard for the basic data and the biometric data.
- b) The MDDS notified for certain other data elements of the socio-economic data may be adopted.
- c) For all other elements, fresh MDDS may be defined.

Authenticity: The Smart Pulse Survey recommended in response to the collection of Socio-economic data may be conducted under the aegis of the Revenue department, including a cross-verification of the veracity of a specified percentage of the records by the supervisory staff of the revenue department. Basing on the same, the revenue officials at the nominated levels will be required to digitally sign the basic data of the records of the SRDH, so as to give them authenticity. A process has also to be put in place for authenticating any changes to the SRDH records.

Legal Sanctity: An appropriate provision may be made in the legislation proposed on Electronic Delivery of Services, on the creation, maintenance and management of the Core Data of People.

Ownership: The Revenue Department shall own the Core Data of People and the ITE&C Department shall manage the same. The Socio-economic Data shall be owned and maintained by the concerned line departments.

Periodicity: The Revenue Department shall conduct the Smart Pulse Survey to collect the Socio-economic Data on a annually over a week to bring the Socio-economic & Aadhaar data up-to-date.

Annexure IV

Salient features of the Aadhaar e-KYC Service

Electronic Know Your Customer or e-KYC is the process, which establishes the identity of a resident, his/her address, date of birth and gender, and provides an instant, electronic and non-repudiable proof of identity and address. It is administered through an ecosystem of KSAs and KUAs. The following are the salient features of e-KYC System.

1. **Paperless:** The eKYC service is fully electronic, and handling of physical documents is eliminated
2. **Consent based:** The KYC data can only be provided upon authorization by the resident through Aadhaar authentication, thus protecting resident privacy.
3. **Eliminates Document Forgery:** Elimination of photocopies of various documents that are currently stored in premises of various stakeholders reduces the risk of identity fraud and protects resident identity
4. **Inclusive:** The fully paperless, electronic, low-cost features make it more inclusive, enabling financial inclusion.
5. **Secure and compliant with the IT Act:** Both end-points of the data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper document. In addition, the use of encryption and digital signature ensures that no unauthorized parties in the middle can tamper or steal the data.
6. **Non-repudiable:** The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the eKYC data makes the entire transaction non-repudiable by all parties involved.
7. **Machine-Readable:** Data provided by SRDH/UIDAI is machine readable, making it possible for the service provider to directly store it as the customer record in their database for purposes of service, audit, etc. without human intervention making the process low cost and error free.
8. **Instantaneous:** The service is fully automated, and Aadhaar data is furnished in real time, without any manual intervention.
9. **Identity:** Establishing identity for purposes such as adding new beneficiaries, confirming genuine beneficiary before service delivery, attendance management, financial transactions etc.
10. **Demand Driven:** Enabling demand-driven, portable service delivery by providing anywhere anytime real-time authentication
11. **MIS:** Access to relevant MIS and empowerment of beneficiary
12. **Transparency:** Improving efficiency & transparency in service delivery by enabling tracking of end-to-end service delivery process, improving accountability and vigilance etc.
13. **Database Cleaning:** Uniqueness attribute can be used to eliminate ghosts & duplicates, if any, from databases. Online authentication for demographic data such as name, address, age/DoB, mobile number and email address can be used for keeping database up to date and clean.
14. **Aadhaar enabled Tracking System:** Provides facility to track various benefits from the Govt. by the respective beneficiaries and timely availing of schemes.

Annexure V

Aadhaar-enabled Payment Systems

(PI See Section 8.7)

Financial inclusion is expected to be a key application of Aadhaar authentication. Adoption of Aadhaar and Aadhaar authentication in Indian banking system is expected to change the financial landscape of the country. To enable same, UIDAI has partnered with various stakeholders including RBI, NPCI, IBA and banks to develop two key Platforms: (i) Aadhaar Payments Bridge (APB) - a system that facilitates seamless transfer of all welfare scheme payments to the beneficiary residents' Aadhaar-enabled Bank Account (AEBA) and (ii) Aadhaar Enabled Payment System (AEPS) - a system that leverages Aadhaar online authentication and enables AEBAAs to be operated in anytime-anywhere banking mode by the marginalized and financially excluded segments of society through a chain of micro-ATMs.

Seeding of Aadhaar number in the bank accounts of residents is a pre-requisite for the AEPS to function effectively.

(V.1) Aadhaar Payments Bridge

APB is a repository of Aadhaar numbers of residents and their primary bank account number used for receiving all social security and entitlement payments from various government agencies. APB requires using Aadhaar number as the primary key for all entitlement payments. This would weed out all fakes and ghosts from the system and ensure that the benefits reach the intended beneficiaries. This benefit has an even greater ramification as more and more social security programs are moving from in-kind to in-cash subsidies.

(V.2) APB Process Steps

The key steps in posting payments via APB are specified below:

1. A service delivery agency that needs to make payments to its beneficiaries (such as MGNREGA wages, scholarships disbursement, old age pension etc.) provides APB File containing details of Aadhaar number, welfare scheme reference number and the amount to be paid to its bank (called sponsor bank).
2. Sponsor bank adds bank IIN (Institute Identification Number provided by NPCI to participant banks) to the APB file and uploads onto NPCI server.

3. NPCI processes uploaded files, prepares beneficiary bank files and generates settlement file, duly linking the Aadhaar number to the primary bank account number of the beneficiary.
4. The settlement file is posted to bank accounts with RBI
5. Destination banks can download the incoming files for credit processing after the settlement file has been processed.

(V.3) Aadhaar Enabled Payment System (AEPS)

The AEPS is intended to address the following field level issues.

A. Technology has to enable the banks to go where the customer is present, instead of the other way around.

B. Technology should allow interoperability among different systems adopted by different banks.

Thus AEPS empowers the marginalised and excluded segments to conduct financial transactions through micro-ATMs deployed by Banks in their area of operation.

(V.4) AEPS Process Steps

The key steps in doing transactions via AEPS are:

1. The resident provides his/her Aadhaar number, the details of financial transaction sought and fingerprint impression at the micro-ATM device.
2. Digitally signed and encrypted data packets are transferred via Bank Switch to NPCI to UIDAI.
3. UIDAI processes the authentication request and communicates the outcome in form of Yes/No response, as in the case of credit card transactions.
4. If the authentication response is yes, the bank carries out the required authorization process and advises micro-ATM on suitable next steps.

(V.5) Benefits of AEPS to Various Stakeholders

Benefits to Residents

1. Obviates need for multiple bank accounts for different schemes
2. Faster channel for receiving all welfare payments without any middle-men
3. Access to micro-ATM in villages saves trips to bank, thus reducing opportunity and travel costs
4. Will help in more usage of formal banking system for managing savings and borrowing
5. Online and interoperable architecture of AEPS ensures anytime, anywhere access of bank accounts which can be a boon, especially for the migrant population
6. Empowerment of individuals especially women

Benefits to Government Departments

7. Use of Aadhaar as primary key eliminates ghost beneficiaries and leads to better targeting
8. Sub-serves goal of furthering Financial Inclusion by processing government disbursements through Aadhaar number Reduces time and cost in payment processing
9. Provide electronic audit trail and end-to-end visibility for all payments

Benefits to Banks

1. Reduces the credit and operational risks in the branchless banking model
2. Enables Banks to rely on BCs to reach the unbanked population
3. Will provide an impetus to electronic payments and thus reduce cash management costs
4. Different financial products through micro-ATMs can be an additional source of revenue for banks and for the BC model

Benefits to RBI

1. Sub-serves goal of furthering Financial Inclusion by processing government disbursements through Aadhaar number
2. Promotes electronification of retail payments through a secure mechanism

Annexure VI

Security and Privacy of personal information

(See Section 11)

1. For the purposes of this policy, personal information includes the Aadhaar Number, the demographic data, the biometric data and the number of a bank account, credit or debit card of a resident, in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.
2. All the departments and agencies in possession of personal information of residents shall undertake the measures prescribed herein in respect of the security and privacy of personal information, to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, fraudulent access, and misuse of personal information.
3. The following **security** measures shall be enforced by all the stakeholders of the AEE.
 - a. Aadhaar data is shared by UIDAI to SRDH through SFTP in encrypted format.
 - b. Aadhaar data is decrypted by SRDH and placed in the AP State Data Center (APSDC).
 - c. SRDH application shall be hosted in APSDC
 - d. APSDC shall be ISO 27001 certified and the certification shall be renewed at the required intervals.
 - e. All the applications deployed to provide services of the SRDH shall be security-audited.
 - f. SRDH shall design and implement an Information Security Management System, in line with the ISO 27005.
 - g. Designate one or more employees to maintain the comprehensive information security program
 - h. Undertake training of employees including temporary or contract employees on all aspects relating to security and privacy of the personal information;
 - i. ensure employee conformance to the policies and safeguards;
 - j. ensure that outgoing employees do not have access to personal information;
 - k. ensure compliance by the 3rd party service providers;
 - l. encryption of personal information stored on portable devices and transported over networks;
 - m. enforce secure user authentication protocols, including a strong password protection mechanism;
 - n. block access to personal information after multiple failed attempts;

4. The following measures shall be enforced by all the stakeholders of the AEE, to ensure the **privacy** of the personal information of residents.
- a. The following principles govern the assurance of the privacy of personal information:
 - i. Notice—residents should be given notice when their data is being collected;
 - ii. Purpose—data should only be used for the purpose stated and not for any other purposes;
 - iii. Consent—data should not be disclosed without the resident's consent;
 - iv. Security—collected data should be kept secure from any potential abuses;
 - v. Disclosure—residents should be informed as to who is collecting their data;
 - vi. Access—residents should be allowed to access their data and make corrections to any inaccurate data; and
 - vii. Accountability—residents should have a method available to them to hold data collectors accountable for not following the above principles.
 - b. Personal information can only be processed in the following circumstances only:
 - i. for specified explicit and legitimate purposes and not in a way incompatible with those purposes;
 - ii. when processing is necessary for the performance of a task carried out in the public interest;
 - iii. when processing is necessary for compliance with a legal obligation;
 - c. Personal information may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
 - d. The personal information must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is deleted or rectified.
 - e. The personal information in the custody of SRDH or any other body, which is a part of the AEE, shall not be transmitted to any other body or person without the appropriate legal authority.

B. SREEDHAR
SECRETARY TO GOVERNMENT